**Web Application Security Assessment**

**ΩREPORT\_NAMEΩ**

DATE

Version: XXX

 Prepared by: **ΩCONSULTANT\_NAMEΩ**

Offensive Security Operations Team (OSOT)

# Table of Content

Table of Content 2

Document Version Control 3

Document History 3

1 Executive Summary 4

1.1 Overview 4

1.2 Total Issues 4

2 Description/Rationale 4

3 Risk Ratings 5

4 Risk Issues Summary 6

5 Detailed findings 7

5.1 πtitleπ 7

Description 7

Details 7

Recommended Countermeasures 7

# Document Version Control

|  |  |
| --- | --- |
| Data Classification: | OFFICIAL-SENSITIVE |
| Client Name: | ΩSHORT\_COMPANY\_NAMEΩ |
| Document Title: | ΩREPORT\_NAMEΩ |
| Author: | ΩCONSULTANT\_NAMEΩ |

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Issue Date | Issued By | Description |
| 0.1 | DATE | ΩCONSULTANT\_NAMEΩ | Draft. Internal only. |
|  |  |  |  |

# 

# Executive Summary

## Overview

The Offensive Security Operations Team was tasked with performing a web application security assessment as part of XXX. XXX provides functionality to allow XXX to do XXX. Of key interest to stakeholders regarding the security of XXX was XXX. During the web application assessment, a number of issues were identified, including XXX. Immediate remediation of XXX is recommended to mitigate the risk of XXX.

## Total Issues

In total, XXX issues were identified during testing:

|  |  |
| --- | --- |
| CVSS Score | Title |
| æreport/findings\_list/findings:::CVSS\_TOTAL>0æ∞cvss\_total∞ | æreport/findings\_list/findings:::CVSS\_TOTAL>0æ∞title∞ |

# Description

Testing was carried out by ΩCONSULTANT\_NAMEΩ. The testing was conducted from XXX to XXX …

**Scope**

The scope of the assessment was to carry out a web application penetration against the XXX application covering mainly but not limited to the OWASP Top 10.

Testing was performed against the following URLs, which are part of the XXX environment:

* XXX

**Credentials**

The following sets of credentials were used as part of testing.

1. Credentials

**Consultant Machine Details:**

The consultant who conducted the test used a machine with the following details:

* External IPv4 address: XXX
* Internal IPv4 address: XXX
* Operating System: Kali Linux

**Caveats**

Some tests were not performed. Some access was not obtained. Some dates were missed. The environment was not ready etc.

**Standards Followed**

The following vulnerability categories (aligned with OWASP Top 10 2017) have been used for web application related findings:

A1:2017 - Injection

A2:2017 - Broken Authentication

A3:2017 - Sensitive Data Exposure

A4:2017 - XML External Entities (XXE)

A5:2017 - Broken Access Control

A6:2017 - Security Misconfiguration

A7:2017 - Cross-Site Scripting (XSS)

A8:2017 - Insecure Deserialization

A9:2017 - Using Components with Known Vulnerabilities

# Risk Ratings

CVSS is a vendor-independent industry open standard, which provides a universal method for rating IT vulnerabilities. It is designed to convey the severity of vulnerabilities, and to help organizations priorities their responses.

It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

Not all vulnerabilities fall within CVSS. Issues that do not fall within the system’s scope are referred to as custom issues and have a risk rating severity of critical, high, medium, low or informational.

|  |  |  |
| --- | --- | --- |
| Rating | CVSSv3 Score | Explanation |
| CRITICAL | 9.0 - 10 | A vulnerability was discovered that has been rated as critical. |
|  |  | This requires resolution as quickly as possible. |
| HIGH | 7.0 - 8.9 | A vulnerability was discovered that has been rated as important. |
|  |  | This requires resolution in the short term |
| MEDIUM | 4.0 - 6.9 | A vulnerability was discovered that has been rated as of medium criticality. |
|  |  | This should be resolved as part of the ongoing security maintenance of the system. |
| LOW | 0.1 - 3.9 | A vulnerability was discovered that has been rated as of low criticality. |
|  |  | This should be addressed as part of routine maintenance tasks |
| NONE | 0 | Good security practices were being followed or an audit item was found to be |
|  |  | present and correct |

# Detailed findings

¬report/findings\_list/findings:::CVSS\_Total>0¬

## πtitleπ

|  |  |
| --- | --- |
| Severity: | Medium |
| CVSSv3 Score: | πCVSS\_totalπ |

### Description

¬overview/paragraph¬ µzzzzµ π.π

ƒparagraphƒ π.π

ƒcodeƒ π.π

ƒitalicsƒ π.π

• ƒbulletƒ π.π

ƒh4ƒ π.π

÷ π.π ≠

### Details

¬poc/paragraph¬ µzzzzµ π.π

ƒparagraphƒ π.π

ƒcodeƒ π.π

ƒitalicsƒ π.π

• ƒbulletƒ π.π

ƒh4ƒ π.π

÷ π.π ≠

### Recommended Countermeasures

¬remediation/paragraph¬ µzzzzµ π.π

ƒparagraphƒ π.π

ƒcodeƒ π.π

ƒitalicsƒ π.π

• ƒbulletƒ π.π

ƒh4ƒ π.π

÷ π.π ≠

**Affected Targets**

¬affected\_hosts/paragraph¬ µzzzzµ π.π

÷ π.π ≠

**CVSSv3 Vector String**

πc3\_vsπ

∆